R. 複合（情報システム／製造）R 社

事業概要	情報システム業、化学品の製造販売等		
従業員数	約 500 人	プライバシーマーク取得	あり
保有個人データ件数	顧客名簿約 40 万件、預かりデータ約 53 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・顧客名簿に 40 万件の個人情報が含まれている。

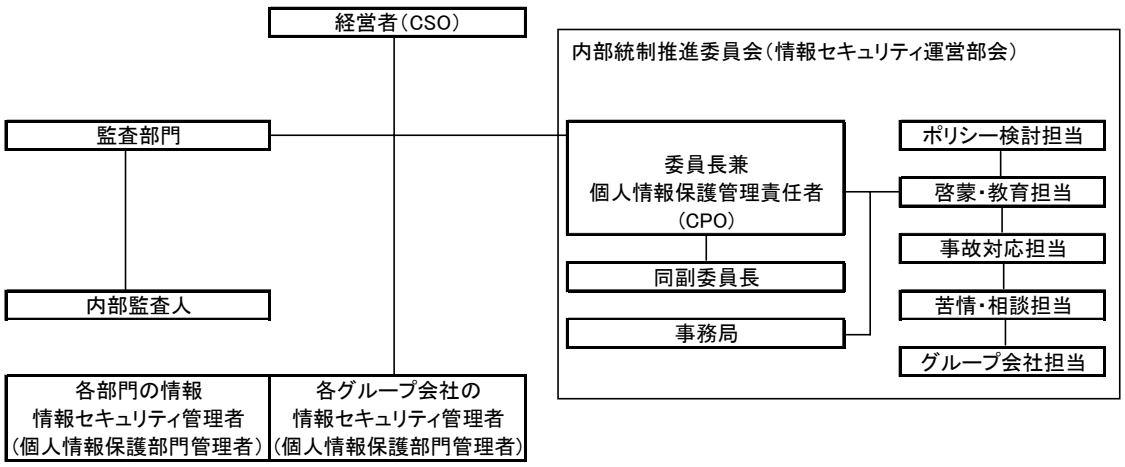
・顧客名簿の個人情報は、会社名、個人名だけでなく、趣味、接待情報、誕生日、家族の誕生日等、営業上知り得た情報についても含まれている。

・テストデータが 1,000 件、顧客から預かったデータは約 53 万件である。

（２）個人情報保護担当部署

・推進室が内部統制推進委員会（情報セキュリティ運営部会）の事務局となっている。

図表　個人情報保護組織図



（３）個人情報保護管理者の有無・位置づけ

・CPO は専務取締役である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマーク、ISO9001、ISO14001、ISMS、BS7799-2 の認証を取得している。

・情報システムインテグレーション及び情報システムアウトソーシング等の事業を通じ、

多くの顧客の個人情報を預かっており、社会的責任が極めて高い。特に情報システムアウトソーシング業務の推進にあたっては、顧客からプライバシーマークの取得を求められるケースが増加した。

・そこで個人情報保護への取組を一層強化し、顧客からの要求に応えるため平成 15 年 5 月よりプライバシーマークの取得に取組んだ。

（５）個人情報保護に向けた取組経緯

・平成 15 年の 7 月に「個人情報保護方針」を制定し、ホームページやパンフレットを用いて社内外に公開した。8 月には JIS 規格に基づき構築した「個人情報保護に関するコンプライアンス・プログラム」の運用を開始した。

・その後、平成 16 年 2 月 24 日にプライバシーマークの認定を受け、平成 17 年 1 月には個人情報保護を含む情報セキュリティ活動の適用範囲をグループ 13 社まで拡大した。

・平成 16 年 8 月に発生した「USB メモリ紛失事故」後、情報資産保護策（HDD パスワード、暗号化、媒体管理の徹底）を追加した。

・個人情報保護法が正式施行された平成 17 年 4 月に、利用目的や取扱方針を追加した「個人情報保護方針」をホームページに公開し、2 年間で規程やガイドラインを延べ 29 文書改版した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・特になし

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・当初は情報システム部門のみの課題であるという認識があり、全社的な協力を得にくかった。経営者が全社体制を一気に作り上げる必要性を感じ、コンサルタントに依頼し、体制づくりをした。

・規程・体制づくりには人件費等含めて約 1 億 2,000 万円要した。この中にはコンサルティング費用も含まれており、コンサルティングに要した費用は約 6,000 万円であった。

・自社 12 部門とグループ会社 14 社の情報セキュリティ管理者が個人情報保護部門管理者として個人情報の管理を実施している。情報セキュリティ運営委員会の事務局の推進室はマネジメントシステムの担当部署であり、2 名で対応している。同社は事業部単位で運営されているが、推進室は部門横断的な組織である。

・月に一度情報セキュリティ運営委員会が開催され、各部門の責任者が参加する。

・情報セキュリティ運営委員会は、ポリシー検討担当、啓蒙・教育担当、事故対応担当、苦情・相談担当、グループ会社担当が委員となっている。それぞれが業務として教育人事、法務の担当者であり、自分の仕事に近い役割を割り当てられているため、本業の延長として取組むことができる。
・毎月実施する会議では、制度変更、事故等の報告や対策などが話し合われている。仮にこの会議内容を外部に依頼するとしたら約 4,000 万円かかるという試算になった。毎月 2～3 時間の会議を実施することによりこのコストを削減できている。

（規程を絞って従業者にわかりやすく説明。常時携帯用のカードも作成）

・規程は全部で 38 あるが、分かりやすい 2 つの規程（「利用者向けガイドライン」と「情報資産取扱ガイドライン」）だけを見ればよい、と従業者には通達し、わかりやすく周知している。
・規程の目的、守るべきこと、事故の連絡ルートなどをまとめた「セキュリティカード」を従業者全員に配布し、常に携帯するようにしている。

（２）個人情報の取得

・独自の個人情報で最も多いものは顧客名簿で約 40 万件である。
・これは営業等で取得する名刺データから作成しているもので、全事業部で利用が可能である。顧客名簿では、会社名、個人名だけでなく、趣味、接待情報、誕生日、家族の誕生日等、営業上知り得た情報についてもデータ化している。

（３）個人情報の利用（第三者提供を含む）

・顧客名簿についてはグループ内で共同利用をし、有効活用を目指している。営業の引き合い段階で過去の営業履歴などを見ることができる。

（従業者は名刺交換の有無により、顧客情報を閲覧できる範囲が異なる）

・従業者によって、顧客名簿の閲覧可能な内容を分けている。従業者が顧客名簿を閲覧する場合、対象と名刺交換をしたことがない場合には会社名、氏名といった名刺情報程度しか見ることができないが、名刺交換をした人の情報についてはより深い情報を見ることができるようになる。
・役員や上級幹部はすべての情報を見ることができる。特定の従業者しか知り得ない情報はデータベースで保管しているが、取得した本人しか見ることができないようになっている。
・データは 1 年に 1 度スクリーニングしており、機微情報と判断されるものについては消去するよう指示している。消去の必要の有無については監査や運営委員会で判断している。

（４）個人情報の管理

①情報の管理体制

（個人情報を集中管理するデータセンターにおいて特に厳重な管理を実施）

・重要情報はすべて、データセンターを持つ事業所で厳重管理している。他拠点の情報のバックアップも当該事業所で管理しており、施錠管理、入退出管理（カード）、監視カメラ、暗証番号と指紋認証によって厳しい管理がなされている。特に重要度の高い情報が管理されているサーバルームへの入室には指紋認証、パスワード入力、IC カードの 3 種類の認証が採用されており、入室は一人ずつしかできない。
・パスワードは月に 1 度変更を義務付けている。
・入退館時には扉が大きな音をたてて開閉するため、人の出入りが警備室等でわかるようになっている。

（ファイル共有ソフトは自己チェックとソフトで二重にチェックを行う）

・従業者が各自のパソコンにファイル共有ソフトが入っていないかどうかを自己チェックし、申告した。その後ウイルスチェックソフトでファイル共有ソフトの有無をチェックした。チェックは毎月実施している。
・ファイル共有ソフトについては、社内掲示板でも呼びかけている。

②従業者への教育方法

・1 年に 1 度集合研修を行っている。顔を合わせた場で説明することにより、制度や個人情報保護の重要性について理解が得られる。
・集合研修以外に新規採用時と階層別研修時にも教育をしている。
・単なる事故事例の紹介だけではなく、社内での事故につながる状況などについて具体的に紹介し理解を深めてもらう。

③盗難対策

・記録媒体は暗号化しないと持ち出せない仕組みになっている。

④ノート PC の安全対策

（持ち出し禁止シールを貼って対応）

・ハードを暗号化しているパソコンには「持ち出し OK」シールを、そうでないものには「持ち出し禁止」シールを貼付し、注意を喚起している。
・800 台あるノート PC のうち 300 台が持ち出し可能である。これらは HDD の暗号化、BIOS ロック、OS、システムで 4 つの ID、パスワードが必要となっている。4 つの ID、パスワードは月に 1 度変更を求めている。パスワードを紙などに記載することは禁止

されている。

⑤外部委託先管理

・個人情報の取扱いは社内で実施することが決められている。社外で委託先が取り扱うことはない。

⑥日常点検・確認の方策

（「レッドカード」を導入し、ゲーム感覚の中で従業者のモチベーションを高める）

・役員や担当がセキュリティ上の危険事項を発見した際に、「レッドカード」を発行している。発行は課単位で集計され、半年ごとに優秀な課には報奨金（1 人 3,000 円程度）が支給される。

⑦初歩的ミスの防止策

・月に一度の情報セキュリティ運営委員会で初歩的ミスの防止について討議している。
・個人情報の漏えいは初歩的ミスが原因であることが多い。事務局が事故を報告し、その原因や対応について具体的に考える。例えば輸送時に事故が起こったケースでは、本来発送すべき人と実際に発送した人が異なっていた。発送者は指定の運送事業者があることを知らず、異なった事業者に依頼して事故につながってしまった。このようなケースを取り上げ、対策について検討していく。
・初歩的ミスの防止として様々なルール作りをしている。“電子メールの CC 配信を上司立会いで実施する”というルールも導入を検討したが、事前の従業者アンケートで業務に支障がでると反対が多かったため見送った。

（５）個人情報の消去・破棄

・紙の情報については少量の場合はシュレッダー、大量の場合は溶解処分としている。
・サーバやパソコン上の情報については消去ソフトを利用している。パソコンを破棄する場合には HDD は破砕している。
・顧客情報については消去していない。いつ利用のチャンスがめぐってくるかわからないからである。例えば、顧客の一人が顧客情報に記載されている会社を退職しても、転職先で顧客となる可能性がないわけではない。その際には履歴を使用して、より良い営業につなげることを企図している。

（６）個人情報の監査

（トップの指示により、年に 4 回の監査を実施）

・専任の監査部門がある。ISMS に詳しい者が監査を行っている。
・この他に内部監査人として社内 33 名、グループ会社 14 名が担当している。内部監査人は、ISO14001 と 9001 の監査ができる人が任命される。
・社長の指示により、監査を年に 2 回から 4 回に増やした。
・個人情報保護の担当者が、今までに 2 回抜き打ちで全事業所を点検している。朝の誰もいない時間帯に訪問し、問題があればレッドカードを発行する。
・自己チェックとして従業者が互いにチェックし合う制度がある。

（７）苦情処理・顧客対応

・従来から顧客窓口は総務部サービス本部が担当しているため、個人情報に関する窓口もサービス本部が担当している。
・開示請求については手順を定めている。手数料は取らないことにしている。基本的に開示請求の対象者となる個人は顧客であり顧客からは手数料を受け取りにくいからである。
・問合せについては電話での対応はしないというルールになっている。そのため電子メールのみ連絡先として掲載している。顧客は電子メールを利用できるので、電子メールのみでも特に問題はない。

（８）事故発生時の対応

・事故発生時には責任者へ報告され、対応が検討される。
・何かあったらすぐに社長へ報告することになっている。

以　上